

JAP20 Rec'd PCT/PTO 03 AUG 2006
明 細 書

情報処理装置および情報処理装置におけるセキュリティ確保方法

5 技 術 分 野

本発明は、情報処理装置および情報処理装置におけるセキュリティ確保方法に関し、特に、1台の情報処理装置を複数のユーザが共有する場合に、個々のユーザが作成したデータのセキュリティを確保する技術に関する。

10 背 景 技 術

パソコンなどの情報処理装置は、複数のユーザによって共有されることが少なくない。このため、パソコンなどの情報処理装置用のオペレーションシステム（以下、単にOSという）も、複数ユーザによって共有されることを前提とした機能を備えている。たとえば、UNIX、Windows XP（登録商標）、
15 Mac OS X（登録商標）などの最近の代表的なOSでは、個々のユーザがシステムの利用開始時にログオン手続（OSによってはログイン手続と呼ばれている）を行い、利用終了時にログオフ手続（OSによってはログアウト手続と呼ばれている）を行うのが基本的な利用形態となっている。

このように複数のユーザが同一の情報処理装置を共有する環境下では、個々のユーザが作成したデータに関して、十分なセキュリティが確保されるような
20 配慮が重要である。たとえば、第1のユーザが作成したデータファイルに対して、第2のユーザが無制限に読み書き可能であるとする、他人には閲覧させたくないファイルや他人には改変されたくないファイルを、共有環境下にある情報処理装置で取り扱うことはできなくなる。

25 そこで、共有環境下にある情報処理装置においても、個々のユーザごとのセキュリティを確保するために、同時に複数のユーザによる重複ログオンが行わ

れることがないような仕組みを採用し、個々のユーザごとにそれぞれ固有のアクセス権限を付与するような運用が行われている。たとえば、特開2003-280781号公報には、個々のユーザごとに異なるアクセス権限を設定しておき、ログオン中のユーザが切り替えられたときに、アクセス権限も切り替

5 るための手法が開示されている。

上述したように、同一の情報処理装置を複数のユーザで共有する場合、個々のユーザごとに固有のアクセス権を設定しておき、所定のアカウントおよびパスワードを用いてログオンしたユーザに対して、当該ユーザに設定されたアクセス権の範囲内でデータファイルへのアクセスを許可する方法が、多くのOS
10 において採用されている。しかしながら、このような方法では、必ずしも十分なセキュリティを確保することはできない。たとえば、多くのOSでは、管理者権限をもった特別なユーザ（たとえば、UNIXにおけるsuper user）の存在が認められており、この特別なユーザとしてログインすれば、何ら制限を受けることなく、すべてのデータファイルにアクセスすることが可能になる。ま
15 た、情報処理装置内にデータファイルが格納されている以上、不正な方法を用いれば、いかなるデータに対してもアクセスすることが可能になる。

そこで本発明は、同一の情報処理装置を複数のユーザで共有する場合、個々のユーザが作成したデータについて、より十分なセキュリティを確保することが可能な方法を提供することを目的とする。

20

発 明 の 開 示

(1) 本発明の第1の態様は、情報処理装置において、

データファイルを格納するためのデータ格納部と、

このデータ格納部に格納されているデータファイルを必要に応じて展開する

25 ためのメモリと、

複数のユーザによる重複ログオンが行われることがないように、所定のユー

ザによるログオン手続が行われた後は、当該ユーザについてのログオフ手続が行われるまで、他のユーザによるログオン手続を拒絶するユーザ管理部と、

ログオン中のユーザの操作に基づいて、データ格納部に格納されている所定のデータファイルをメモリ上に展開するファイル展開処理と、メモリ上に展開
5 されている所定のデータファイルをデータ格納部に格納するファイル保存処理と、を実行する展開保存部と、

ログオン中のユーザの操作に基づいて、所定のアプリケーションプログラムを実行し、メモリ上に新たなデータファイルを作成する処理もしくはメモリ上に展開されている既存のデータファイルに対する更新処理を実行するプログラ
10 ム実行部と、

特定のユーザがログオフ手続を実行したときに、データ格納部に格納されているデータファイルのうち、当該特定のユーザの作業に基づいて作成もしくは更新されたデータファイルの全部もしくは所定の一部を退避対象ファイルとして認識する退避対象認識処理と、退避対象ファイルをネットワークを介して外
15 部の記憶装置にコピーすることにより退避させる退避処理と、データ格納部内に格納されている退避対象ファイルを削除する削除処理と、外部の記憶装置に退避された退避対象ファイルをデータ格納部内にコピーして復元するために必要な管理情報を作成する管理情報作成処理と、作成した管理情報を外部の記憶場所に保存する管理情報保存処理と、を実行する退避処理部と、

20 上記特定のユーザがログオン手続を実行した後、必要に応じて、管理情報を参照することにより、外部の記憶装置に退避されている退避対象ファイルをデータ格納部内にコピーして復元する復元処理を実行する復元処理部と、
を設けるようにしたものである。

(2) 本発明の第2の態様は、上述の第1の態様に係る情報処理装置において、
25 復元処理部が、データファイルの保存時の階層構造を復元する予備復元処理と、この予備復元処理によって復元された階層構造内から選択された特定のデ

ータファイルを復元する本復元処理と、を実行するようにしたものである。

(3) 本発明の第3の態様は、上述の第1または第2の態様に係る情報処理装置において、

5 退避処理部が、予め定められた退避対象フォルダ内に格納されているデータファイルを、退避対象ファイルとして認識するようにしたものである。

(4) 本発明の第4の態様は、上述の第1または第2の態様に係る情報処理装置において、

退避処理部が、予め定められた所定の拡張子がファイル名に付されているデータファイルを、退避対象ファイルとして認識するようにしたものである。

10 (5) 本発明の第5の態様は、上述の第1～第4の態様に係る情報処理装置において、

退避処理部が、管理情報保存処理を実行する際に、着脱自在な携帯可能情報記録媒体に管理情報を保存し、

15 復元処理部が、復元処理を実行する際に、この携帯可能情報記録媒体に保存されている管理情報を参照するようにしたものである。

(6) 本発明の第6の態様は、上述の第1～第5の態様に係る情報処理装置において、

管理情報として、退避対象ファイルの退避先となる外部の記憶装置のアドレス情報を用いるようにしたものである。

20 (7) 本発明の第7の態様は、上述の第1～第6の態様に係る情報処理装置において、

退避処理部が、退避処理を実行する際に、退避対象ファイルを所定の分割方法に基づいて複数の分割ファイルに分割し、個々の分割ファイルをそれぞれ異なる複数の記憶装置に退避させる処理を実行し、この所定の分割方法を示す情報
25 報を含む管理情報を作成するようにし、

復元処理部が、管理情報に含まれている分割方法を示す情報に基づいて、退

避対象ファイルの復元を行うようにしたものである。

(8) 本発明の第8の態様は、上述の第1～第7の態様に係る情報処理装置において、

5 退避処理部が、退避処理を実行する際に、退避対象ファイルを所定の暗号化方法に基づいて暗号化した上で外部の記憶装置に退避させる処理を実行し、この所定の暗号化方法を示す情報を含む管理情報を作成するようにし、

復元処理部が、管理情報に含まれている暗号化方法を示す情報に基づいて復号化処理を実行し、退避対象ファイルの復元を行うようにしたものである。

10 (9) 本発明の第9の態様は、上述の第1～第8の態様に係る情報処理装置において、

退避処理部が、削除処理を実行する際に、メモリに展開されている退避対象ファイルに対しても削除する処理を行うようにしたものである。

15 (10) 本発明の第10の態様は、上述の第1～第9の態様に係る情報処理装置としてコンピュータを機能させるコンピュータプログラムを用意し、このプログラムをコンピュータ読取り可能な記録媒体に記録して配付できるようにしたものである。

(11) 本発明の第11の態様は、

データファイルを格納するためのデータ格納部と、

20 このデータ格納部に格納されているデータファイルを必要に応じて展開するためのメモリと、

複数のユーザによる重複ログオンが行われないように、所定のユーザによるログオン手続が行われた後は、当該ユーザについてのログオフ手続が行われるまで、他のユーザによるログオン手続を拒絶するユーザ管理部と、

25 ログオン中のユーザの操作に基づいて、データ格納部に格納されている所定のデータファイルをメモリ上に展開するファイル展開処理と、メモリ上に展開されている所定のデータファイルをデータ格納部に格納するファイル保存処理

と、を実行する展開保存部と、

ログオン中のユーザの操作に基づいて、所定のアプリケーションプログラムを実行し、メモリ上に新たなデータファイルを作成する処理もしくはメモリ上に展開されている既存のデータファイルに対する更新処理を実行するプログラ

5 ム実行部と、

を備える情報処理装置を、複数のユーザで共用する場合に、個々のユーザごとにデータのセキュリティを確保する方法において、

特定のユーザがログオフ手続を実行したときに、データ格納部に格納されているデータファイルのうち、当該特定のユーザの作業に基づいて作成もしくは

10 更新されたデータファイルの全部もしくは所定の一部を退避対象ファイルとして認識する退避対象認識処理と、退避対象ファイルをネットワークを介して外部の記憶装置にコピーすることにより退避させる退避処理と、データ格納部内に格納されている退避対象ファイルを削除する削除処理と、外部の記憶装置に退避された退避対象ファイルをデータ格納部内にコピーして復元するために必要な管理情報を作成する管理情報作成処理と、作成した管理情報を外部の記憶場所

15 場所に保存する管理情報保存処理と、を実行する退避処理段階と、

上記特定のユーザがログオン手続を実行した後、必要に応じて、管理情報を参照することにより、外部の記憶装置に退避されている退避対象ファイルをデータ格納部内にコピーして復元する復元処理を実行する復元処理段階と、

20 を情報処理装置に行わせるようにしたものである。

(12) 本発明の第12の態様は、上述の第11の態様に係る情報処理装置におけるセキュリティ確保方法において、

復元処理段階が、データファイルの保存時の階層構造を復元する予備復元段階と、この予備復元段階によって復元された階層構造内から選択された特定の

25 データファイルを復元する本復元段階と、によって構成されるようにしたものである。

(13) 本発明の第 1 3 の態様は、上述の第 1 1 または第 1 2 の態様に係るセキュリティ確保方法における退避処理段階および復元処理段階をコンピュータに実行させるコンピュータプログラムを用意し、このプログラムをコンピュータ読取り可能な記録媒体に記録して配付できるようにしたものである。

- 5 本発明に係る情報処理装置および情報処理装置におけるセキュリティ確保方法によれば、個々のユーザがログオフする時点で、セキュリティ確保が必要な退避対象ファイルが外部の記憶装置へ退避され、データ格納部からは削除されてしまうため、退避対象ファイルは情報処理装置内には残らなくなる。したがって、当該情報処理装置が複数のユーザによって共有されていたとしても、
10 十分なセキュリティを確保することが可能になる。

図 面 の 簡 単 な 説 明

図 1 は、本発明の一実施形態に係る情報処理装置 1 0 0 の運用状態を示すブロック図である。

- 15 図 2 は、図 1 に示す情報処理装置 1 0 0 におけるデータ格納部 1 1 0 内に格納されたデータファイルの階層構造を示すウィンドウ表示の一例を示す図である。

- 図 3 は、図 1 に示す情報処理装置 1 0 0 に関するものであり、図(a) は退避処理前のデータ格納部 1 1 0 の状態を示す図、図(b) は退避処理後のデータ格納部
20 1 1 0 および外部の記憶装置 3 0 0 の状態を示す図である。

図 4 は、図 1 に示す情報処理装置 1 0 0 の復元処理部 1 7 0 による二段階の復元処理機能の概念を示す図である。

図 5 は、退避対象ファイルに対する分割処理の概念を示す図である。

- 図 6 は、退避対象ファイルに対する分割処理を行うために、ネットワーク 2
25 0 0 に 3 つの異なる記憶装置を接続した変形例を示すブロック図である。

発明を実施するための最良の形態

以下、本発明を図示する実施形態に基づいて説明する。

<<< § 1. 情報処理装置の基本構成 >>>

図 1 は、本発明の一実施形態に係る情報処理装置 1 0 0 の運用状態を示すブ
5 ロック図である。図 1 において、一点鎖線で囲った部分が本発明に係る情報処
理装置 1 0 0 である。図示のとおり、この情報処理装置 1 0 0 は、データ格納
部 1 1 0、展開保存部 1 2 0、メモリ 1 3 0、ユーザ管理部 1 4 0、プログラ
ム実行部 1 5 0、退避処理部 1 6 0、復元処理部 1 7 0 によって構成されてい
る。これらの各構成要素のうち、データ格納部 1 1 0、展開保存部 1 2 0、メ
10 モリ 1 3 0、ユーザ管理部 1 4 0、プログラム実行部 1 5 0 は、従来の一般的
な情報処理装置 1 0 0 に備わっている構成要素であり、退避処理部 1 6 0 およ
び復元処理部 1 7 0 が、本発明に特有の構成要素になる。

情報処理装置 1 0 0 は、いわゆるコンピュータによって構成される装置であ
り、ここでは、特に、汎用のパソコンによって情報処理装置 1 0 0 を構成した
15 例を述べることにする。データ格納部 1 1 0 は、データファイルを格納するた
めの構成要素であり、パソコンの場合、内蔵もしくは外付けのハードディスク
装置によって構成されるのが一般的である。もちろん、光磁気ディスク装置や
書換え可能な光ディスク装置（CD-RAM 装置など）によってデータ格納部
1 1 0 を構成することも可能である。一方、メモリ 1 3 0 は、データ格納部 1
20 1 0 に格納されているデータファイルを必要に応じて展開するための構成要素
であり、通常、RAM によって構成される。

データ格納部 1 1 0 がデータファイルの格納場所として機能するのに対し、
メモリ 1 3 0 はデータファイルに対する作業場所として機能する。展開保存部
1 2 0 は、必要に応じて、データ格納部 1 1 0 に格納されている所定のデータ
25 ファイルをメモリ 1 3 0 上に展開するファイル展開処理と、メモリ 1 3 0 上に
展開されている所定のデータファイルをデータ格納部 1 1 0 に格納するファイ

ル保存処理と、を実行する構成要素である。パソコンを情報処理装置100として用いた場合、展開保存部120は、OSプログラムの機能の一部として実現されることになる。

ユーザが、アプリケーションプログラムによって、データ格納部110内の

5 データファイルに対して所定の処理作業を実行する際には、まず、展開保存部120のファイル展開処理によって、データ格納部110内の作業対象となるデータファイルが、メモリ130上に展開される。この作業は、通常、アプリケーションプログラムによって、作業対象となるデータファイルを開く処理として実行される。図1には、データ格納部110に格納されている3つのデータ

10 ファイルF1～F3のうちのファイルF2を開く操作が行われた状態が示されている。データ格納部110内に格納されていたデータファイルF2は、メモリ130上に展開された状態となっている。

プログラム実行部150は、所定のアプリケーションプログラムを実行し、メモリ130上に展開されている既存のデータファイルに対する更新処理を実

15 行する機能を有する。図示の例の場合、プログラム実行部150は、メモリ130上に展開されているデータファイルF2に対して所定の更新処理を実行することになる。データファイルF2に対して加えられる更新処理の内容は、アプリケーションプログラムの種類やユーザが実行する操作によって様々である。結局、プログラム実行部150は、所定のアプリケーションプログラムを格納

20 する手段と、これを実行するための演算処理手段によって構成されることになる。

上述したとおり、メモリ130は、データファイルに対する作業場所として機能する構成要素であり、アプリケーションプログラムによる作業対象となるデータファイルを一時的に保持する役割しか果たさない。したがって、メモリ

25 130上で所定の作業が完了したデータファイルは、再びデータ格納部110へと格納される。この作業は、通常、アプリケーションプログラムによって、

作業対象となるデータファイルを保存する処理として実行される。この場合、元のファイル名と同一のファイル名で保存すると、いわゆる上書き保存がなされ、別なファイル名で保存すると、新たなデータファイルとしての保存がなされる。たとえば、図示の例において、メモリ130上に展開されているデータ

- 5 ファイルF2に対する作業が完了し、更新処理がなされた場合、これを「F2」なる同一のファイル名で保存すると、データ格納部110内のデータファイルF2は、メモリ130上の更新されたデータファイルF2に置き換えられることになるが（上書き保存）、たとえば、「F4」などの別なファイル名で保存すると、データ格納部110内に格納されていたデータファイルF2はそのまま
10 の状態で、新たに「F4」なるファイル名のデータファイルが追加される。

- なお、プログラム実行部150は、所定のアプリケーションプログラムの実行により、メモリ130上に新たなデータファイルを作成する処理を行う機能も有している。この機能は、通常、アプリケーションプログラムによる新規ファイルの作成作業として実行される。こうしてメモリ130上に新規作成され
15 たデータファイルは、最終的には、保存処理によって、データ格納部110内に保存されることになる。

- 結局、展開保存部120によるデータ展開処理やデータ保存処理、プログラム実行部150による所定のアプリケーションプログラムの実行処理は、いずれも情報処理装置100に対するユーザの入力操作に基づいて行われるが、複数のユーザによる共用を前提とした情報処理装置100の場合、個々のユーザ
20 はそれぞれ所定のログオン手続を行うことにより情報処理装置100に対する作業を開始し、所定のログオフ手続を行うことにより情報処理装置100に対する作業を終了することになる。ここで、「ログオン」とは、所定のユーザが所定のアカウント（ユーザ名）および必要に応じて所定のパスワードを入力して、
25 情報処理装置100に対する利用状態を確保することを言い、「ログオフ」とは、現在ログオン中のユーザの利用状態を終了させることを言う。なお、OSによ

っては、「ログオン」の代わりに「ログイン」なる文言を用い、「ログオフ」の代わりに「ログアウト」なる文言を用いる場合もあるが、本明細書において両者は同義である。また、OSによっては、ログオフ手続を行うことなしに、シャットダウン操作（OSの機能を終了させ、電源を切る操作）が可能なものもあるが、本明細書にいうログオフ手続とは、このようなシャットダウン操作により利用状態を終了させる手順も含むものである。

ユーザ管理部140は、複数のユーザによる重複ログオンが行われることがないように、所定のユーザによるログオン手続が行われた後は、当該ユーザについてのログオフ手続が行われるまで、他のユーザによるログオン手続を拒絶するユーザ管理を行う構成要素である。最近のパソコン用OSには、このユーザ管理部140の機能が、OSプログラムの機能の一部として標準装備されている。

なお、この実施形態の場合、ユーザ管理部140は、重複ログオンが行われることがないようなユーザ管理を行うだけでなく、現在ログオン中のユーザに対するアクセス権の管理も行う機能を有している。すなわち、ユーザ管理部140は、予め複数のユーザについてのアクセス権限を登録する機能を有しており、現時点でログオンしているユーザが誰であることを認識し、展開保存部120およびプログラム実行部150に対して、当該ユーザのアクセス権の範囲内での処理動作のみを許可する監督処理を行う。たとえば、他のユーザが作成したデータファイルに対する読み書きの権限が一切与えられていないユーザがログオンしている場合、他のユーザが作成したデータファイルを展開しようとする展開保存部120の処理動作はユーザ管理部140によって許可されないことになる。同様に、他のユーザが作成したデータファイルに対する読み出し権限は与えられているが、書き込みの権限が与えられていないユーザがログオンしている場合、他のユーザが作成したデータを改変しようとするプログラム実行部150の処理動作、あるいは、改変後のデータをデータ格納部110に上

書き保存する展開保存部120の処理動作は、ユーザ管理部140によって許可されないことになる。

以上、情報処理装置100の構成要素のうち、データ格納部110～プログラム実行部150までの機能を説明したが、これら5つの構成要素の各機能は、
5 いずれも最近のパソコン用OSが標準的に備えている機能であり、これら5つの構成要素を備える情報処理装置100は、最近のOS（たとえば、Windows XP（登録商標）、Mac OS X（登録商標）、UNIXなど）を組み込んだ標準的なパソコンというべきものである。そして、この標準的なパソコンでは、OSが、複数ユーザによる共用を前提として設計されているため、上述
10 のように、利用を開始するユーザには、所定のユーザ名によるログオン手続が原則的には要求され、当該ユーザ名の下で設定されたアクセス権の範囲内で、個々のデータファイルへのアクセスが許可されることになる。

しかしながら、既に述べたとおり、このような方法では、必ずしも十分なセキュリティを確保することはできない。たとえば、UNIXにおけるsuper user
15 のような管理者権限をもった特別なユーザとしてログインすれば、何ら制限を受けることなく、すべてのデータファイルにアクセスすることが可能になる。また、データ格納部110内にデータファイルが格納されている以上、不正な方法を用いれば、いかなるデータファイルに対してもアクセスすることは可能である。

20 <<< § 2. 本発明の基本的な特徴 >>>

本発明の目的は、§ 1で述べたように、同一の情報処理装置100を複数のユーザで共有する場合、個々のユーザが作成したデータについて、より十分なセキュリティを確保することにある。そのため、本発明に係る情報処理装置100には、退避処理部160および復元処理部170という本発明に固有の構成要素が付加されている。また、本発明を実施する上では、情報処理装置10
25 0をネットワーク200に接続し、このネットワーク200に接続された外部

の記憶装置300を利用できる環境が必要である。

もっとも、現在、パソコンなど情報処理装置100は、ネットワーク200に接続して利用するのが一般的になりつつあるので、多くの情報処理装置100には、既にネットワーク200への接続環境が整っていることになる。ネットワーク200としては、社内LANなどのローカルなネットワークを利用してもよいし、インターネットを利用してもかまわない。また、外部の記憶装置300としては、このネットワーク200を介してアクセス可能な記憶装置であれば、どのような装置を用いてもかまわない。一般的には、データサーバやバックアップサーバなどのサーバ装置を外部の記憶装置300として用いると便利である。結局、パソコンなど、既存の情報処理装置100の多くは、既に、ネットワーク200を介して外部の記憶装置300へアクセスする環境下にあるのが一般的であり、そのような情報処理装置100については、既存の環境をそのまま利用して本発明の実施が可能である。

一方、本発明を実施する上では、情報処理装置100外に管理情報を記憶させる記憶場所を用意しておく必要がある。図1に示す例では、携帯可能情報記録媒体400を、この記憶場所として利用している。具体的には、この実施形態の場合、ICカードを携帯可能情報記録媒体400として用いている。ICカードにアクセスを行う場合、通常、専用のリーダライタ装置が必要になるので、この実施形態では、情報処理装置100として用いるパソコンに、リーダライタ装置を接続し、このリーダライタ装置にICカードを挿入することにより、パソコンからのアクセスが可能になるようにしている。もちろん、ICカードは、着脱自在な携帯可能情報記録媒体400であり、随時、リーダライタ装置から抜き出して携帯することが可能である。

結局、本発明を実施するために、情報処理装置100の内部に新たに設けた構成要素は、退避処理部160と復元処理部170ということになる。本発明の基本概念は、特定のユーザがログオフ手続を実行する際に、当該特定のユー

5 ザがデータ格納部110内に保存したデータファイルを、外部の記憶装置300へと退避させ、データ格納部110内のデータファイルを削除してしまうことにある。退避処理部160は、この退避のための処理を実行する構成要素である。この退避処理により、当該ユーザが作成したデータファイルは、情報処理装置100内から削除されて存在しなくなってしまうため、後に、別なユーザが同じ情報処理装置100にログオンした場合でも、十分なセキュリティが確保できることになる。もちろん、当該特定のユーザが再度ログオンしたときには、外部の記憶装置300に退避させていたデータファイルをデータ格納部110内へ復元する必要がある。復元処理部170は、この復元処理を行う構成要素である。以下、退避処理部160の機能および復元処理部170の機能を詳述する。

15 退避処理部160は、図1に示されているとおり、5つの処理機能を有している。いずれの処理も、現在ログオン中のユーザがログオフを実行したときに実行されることになる。前述したとおり、ユーザのログオンおよびログオフ手続は、ユーザ管理部140によって処理される。ユーザ管理部140は、現在ログオン中のユーザがログオフ手続を実行した場合、その旨を退避処理部160へ報告し、この5つの処理機能の実行を促すことになる。

20 退避処理部160で最初に実行される退避対象認識処理は、特定のユーザがログオフ手続を実行したときに、データ格納部110に格納されているデータファイルのうち、当該特定のユーザの作業に基づいて作成もしくは更新されたデータファイルの全部もしくは所定の一部を退避対象ファイルとして認識する処理である。たとえば、図示の例において、現在ログオン中のユーザを「ユーザ甲」と呼ぶことにし、このユーザ甲のログオン中の作業に基づいて、3つのデータファイルF1、F2、F3が作成もしくは更新されたものとしよう。この場合、図示のとおり、データ格納部110内には、3つのデータファイルF1、F2、F3が格納された状態になっている。ここで、ユーザ甲の作業に基

づいて作成もしくは更新されたデータファイルの全部を退避対象ファイルとして認識することにしておけば、図示の例の場合、ユーザ甲がログオフ手続を実行したとき、データ格納部110内に格納されている3つのデータファイルF1, F2, F3のすべてが、退避対象ファイルとして認識されることになる。

- 5 退避処理部160で実行される第2の処理は、この退避対象ファイルをネットワーク200を介して外部の記憶装置300にコピーすることにより退避させる退避処理である。上述の例の場合、データ格納部110内に格納されている3つのデータファイルF1, F2, F3のすべてが、退避対象ファイルとして認識されているので、この3つのデータファイルF1, F2, F3のすべて
- 10 が、ネットワーク200を介して外部の記憶装置300へとコピーされることになる。このコピー処理自体は、いわばバックアップ処理と同等の作業になる。

- 退避処理部160で実行される第3の処理は、データ格納部110内に格納されている退避対象ファイルを削除する削除処理である。この削除処理を伴う点が、一般的なバックアップ処理と異なる点である。上述した退避処理により、
- 15 退避対象ファイルF1, F2, F3が外部の記憶装置300へコピーされたわけであるが、この削除処理により、コピー元となったデータ格納部110内のオリジナルの退避対象ファイルF1, F2, F3が削除されることになるので、結果的に、上述した退避処理は、バックアップとしての意味はもたないことになる。

- 20 なお、一般に、ハードディスク装置などのデータ格納部110に格納されているデータファイルを削除する方法として、当該データファイルをそのディレクトリ上において削除する方法（ディレクトリを書き換えることにより、ディレクトリ上は当該ファイルが存在していないこととする方法）と、実際のデータ記録領域に別なデータを上書きすることによりデータファイル自身を完全に
- 25 削除する方法と、が知られているが、本発明を実施する上では、いずれの方法を採ってもかまわない。前者の方法よりも後者の方法の方が、より高いセキュ

リティを確保する上では好ましいが、削除処理の負担という点では、前者の方法の方が後者の方法よりも負担が軽くなる。

退避処理部160で実行される第4の処理は、外部の記憶装置300に退避された退避対象ファイルを、将来、データ格納部110内にコピーして復元するために必要な管理情報を作成する管理情報作成処理である。ここで作成する管理情報は、外部の記憶装置300に退避された退避対象ファイルをデータ格納部110内にコピーして復元することが可能な情報であれば、どのような形態の情報でもかまわないが、一般的には、退避対象ファイルの退避先となる外部の記憶装置300のアドレス情報を管理情報として用いるようにすればよい。たとえば、ネットワーク200としてインターネットを用い、外部の記憶装置300として、インターネットに接続されたデータサーバを用いた場合、このデータサーバ上での退避対象ファイルのURLアドレスを管理情報として用いるようにすればよい。上述の例の場合、退避処理により、退避対象ファイルF1、F2、F3は、外部の記憶装置300内の所定の退避場所にコピーされることになるので、この退避場所を示すURLアドレスを管理情報として作成すればよい。なお、実用上は、この管理情報には、ユーザ甲のログオフ手続で作成された管理情報であることを示す情報を含ませしておくのが好ましい。

退避処理部160で実行される第5の処理は、作成された管理情報を外部の記憶場所に保存する管理情報保存処理である。図1に示す例では、管理情報を保存するための外部の記憶場所として、携帯可能情報記録媒体400（具体的にはICカード）を用意している。したがって、管理情報は、この携帯可能情報記録媒体400内に保存されることになる。ログオフ手続を完了したユーザ甲は、最後に、この携帯可能情報記録媒体400を、情報処理装置100から取り外して携帯する。具体的には、情報処理装置100としてのパソコンに接続されたリーダライタ装置から、携帯可能情報記録媒体400としてのICカードをエジェクトして取り出す作業を行うことになる。

以上の各処理により、ユーザ甲のログオフ手続は完了である。このようなログオフ手続を経た結果、ユーザ甲がログオン中に作業したデータファイルF 1, F 2, F 3は、データ格納部110内から削除された状態になっている。したがって、この後、第2のユーザ乙が情報処理装置100に対するログオン手続を行なったとしても、ユーザ乙は、ユーザ甲が作業したデータファイルF 1, F 2, F 3にアクセスすることはできない。たとえユーザ乙が、管理者権限をもつ特別なユーザであっても、あるいは、不正な手段でアクセスを行なったとしても、そもそもデータファイルF 1, F 2, F 3は、データ格納部110内には存在しないのであるから、物理的にアクセスすることはできない状態になっている。

もちろん、厳密な意味でアクセス不能にするためには、上述したとおり、データ格納部110内の実際のデータ記録領域に別なデータを上書きすることによりデータファイル自身を完全に削除する方法を採るのが好ましい。なお、ユーザ甲がログオフした時点で、メモリ130内にデータが展開されたままになっていたとしても、通常、当該データに対する作業を実行したアプリケーションプログラムが終了された時点で、当該データに対する通常の方法によるアクセスは不可能になるので、後にログオンした別なユーザ乙が、メモリ130内に残っていたデータファイルにアクセスすることは困難である。ただ、より高度なセキュリティを確保する必要がある場合には、退避処理部160が、データ格納部110内の退避対象ファイルに対して削除処理を実行する際に、メモリ130に展開されている退避対象ファイルに対しても削除する処理を行うようにすればよい。図示の例の場合、メモリ130上に展開されているデータファイルF 2に対する削除処理が併せて行われることになる。具体的には、メモリ130を構成するRAM領域に、ランダムなデータを上書きする作業を実行すればよい。

もちろん、この第2のユーザ乙がログオフ手続を行う際にも、全く同様の手

順が実行される。すなわち、ユーザ乙の作業によりデータ格納部110内に作成された退避対象ファイルは、退避処理部160により、外部の記憶装置300内の所定のアドレス場所にコピーされた後、データ格納部110内のオリジナルファイルは削除されることになる。このとき、復元に必要な管理情報が作成されることになるが、この管理情報は、ユーザ乙用の携帯可能情報記録媒体400（ICカード）に保存されることになる。

このように、ここに示す実施形態では、情報処理装置100を共用する各ユーザは、それぞれ固有の携帯可能情報記録媒体400（ICカード）を所持しており、情報処理装置100に対するログオン手続を行う前に、この携帯可能情報記録媒体400を情報処理装置100に接続した状態とし（リーダライタ装置にICカードを挿入した状態とし）、ログオフ手続を完了した際には、この携帯可能情報記録媒体400を情報処理装置100から取り外した状態とする（リーダライタ装置からICカードをエジェクトした状態とする）。

結局、本発明では、特定のユーザがログオン中に作業したデータファイルを、当該特定のユーザのログオフ手続によって、情報処理装置100内から削除してしまうことができるため、同一の情報処理装置100を複数のユーザで共用する場合であっても、別のユーザが作業したファイルへのアクセスは、どのようなアクセス権限をもったユーザであっても不可能になる。このため、個々のユーザが作成したデータについて、十分なセキュリティを確保することが可能になる。

もともと、各ユーザが、再度ログオン手続を行い、情報処理装置100を利用して、過去に作業したデータファイルの内容を閲覧したり、更新したりする際には、退避したデータファイルをデータ格納部110へ復元する処理を行う必要がある。たとえば、上述の例において、第2のユーザ乙がログオフ手続を行った後、再び第1のユーザ甲がログオン手続を行った場合を考えよう。この場合、退避対象ファイルF1，F2，F3を、外部の記憶装置300からデー

- タ格納部110へと復元する処理を行う必要がある。このような復元処理を行う構成要素が、復元処理部170である。すなわち、復元処理部170は、特定のユーザがログオン手続を実行した後、携帯可能情報記録媒体400内の管理情報を参照することにより、外部の記憶装置300に退避されている退避対象ファイルデータをデータ格納部110内にコピーして復元する復元処理を実行する。

- 上述したとおり、ここに示す実施形態では、個々のユーザは、それぞれ固有の携帯可能情報記録媒体400（ICカード）を所持しており、情報処理装置100に対するログオン手続を行う前に、この携帯可能情報記録媒体400を情報処理装置100に接続した状態にする。たとえば、ユーザ甲が情報処理装置100に対してログオン手続を行う際には、所持していたICカードをリーダライタ装置に挿入する作業を行うことになる。ユーザ管理部140は、ユーザ甲からのログイン手続を認識すると、その旨を復元処理部170に報告し、復元処理部170による復元処理の実行を促す。復元処理部170は、携帯可能情報記録媒体400（ユーザ甲が挿入したICカード）内の管理情報を参照することにより、前回のログオフ時に退避させられた退避対象ファイルF1，F2，F3の退避場所アドレス（外部の記憶装置300内の所定アドレス）を認識し、これらのファイルをデータ格納部110内にコピーして復元する処理を実行する。

- このような復元処理が実行されれば、データファイルF1，F2，F3は、再びデータ格納部110内に格納された状態となるので、ユーザ甲は、必要に応じて、これらのデータファイルをメモリ130上に展開させた上で、プログラム実行部150による更新処理を実行することができる。もちろん、ユーザ甲が再びログオフ手続を行えば、データファイルF1，F2，F3は、再び外部の記憶装置300へと退避させられ、データ格納部110内からは削除されることになる。

実用上は、退避処理部160による退避処理は、ユーザがログオフ手続を行

ったときに自動的に行われるようにし、復元処理部170による復元処理は、ユーザがログオン手続を行ったときに自動的に行われるようにしておくのが好ましい。そうすれば、退避処理や復元処理は、ユーザが何ら意識しない状態で行われることになり、本発明の特徴となる退避処理部160や復元処理部170の動作は、ユーザの関知しない裏の動作ということになる。本発明の特徴は、パソコンなどの既存の情報処理装置に、退避処理部160および復元処理部170を付加した点にあるが、少なくとも一般のユーザから見れば、本発明を適用したパソコンの操作性は、既存のパソコンと何ら変わることはない。

なお、外部の記憶装置300内からデータファイルの復元を行った場合、外部の記憶装置300内の復元対象となったデータファイルは削除してもよいし、そのまま残しておいてもかまわない。外部の記憶装置300の記憶容量をできるだけ節約したい場合には、復元処理部170による復元処理が行われたデータファイルについては、外部の記憶装置300内から削除する処理を行えばよい。あるいは、復元処理が行われた後も、外部の記憶装置300内のデータファイルをそのまま残しておき、次回、同じファイル名のデータファイルについて再度の退避処理を行う際に、前回との差分データのみをコピーするような方法を探ることも可能である。

<<< § 3. いくつかの実用的な工夫 >>>

上述の§2では、本発明の基本的な実施形態を説明した。ここでは、本発明を実施する上で、より実用的ないくつかの工夫を述べる。

(1) 退避対象ファイルの選択

上述した基本的な実施形態では、特定のユーザ甲がログオフ手続を実行したときに、データ格納部110に格納されているデータファイルのうち、特定のユーザ甲の作業に基づいて作成もしくは更新されたデータファイルの全部を退避対象ファイルとして認識するようにはしていたが、全部ではなく所定の一部を選択して、退避対象ファイルとして認識するようにはしてもかまわない。これは、

通常、すべてのデータファイルについて等しくセキュリティを確保する必要があるとは限らないからである。

ユーザの作業対象となったデータファイルのうちの一部のみを退避対象ファイルとするには、予め退避対象ファイルとして選択するための基準を定めてお
5 けばよい。たとえば、予め所定のフォルダを退避対象フォルダとして定めてお
き、退避処理部160が退避対象認識処理を行う際に、この退避対象フォルダ
内に格納されているデータファイルを、退避対象ファイルとして認識するよう
にすればよい。

図2は、データ格納部110内に格納されたデータファイルの階層構造を示
10 すウィンドウ表示の一例を示す図である。図示の例では、左側のウィンドウW
1に、データ格納部110内の階層構造の全体像が示されており、右側のウイ
ンドウW2には、左側のウィンドウW1上で選択された特定のフォルダB（図
では、ハッチングにより選択状態を示している）の内容が示されている。この
例では、データ格納部110全体が「C」なるボリュームで示されており、そ
15 の直下に、フォルダA、B、Cなる3つのフォルダが作成されている。そして、
フォルダAにはファイルF0が格納され、フォルダBにはファイルF1、F2、
F3が格納され、フォルダCにはファイルF4、F5が格納されている。

ここで、たとえば、フォルダAに格納されているファイルF0が、OSに関
連して利用されるデータファイルであるとし、他のユーザにアクセスされても、
20 セキュリティ上は問題がないものとしよう。また、フォルダCに格納されてい
るファイルF4、F5は、ユーザ甲が所定のアプリケーションプログラムで作
成したデータファイルであるが、これらのファイルも、その性質上、セキュリ
ティ上の問題がないものとしよう。この場合、セキュリティ上、問題が生じる
ファイルは、フォルダBに格納されているファイルF1、F2、F3だけとい
25 うことになる。

このような場合は、予め、フォルダBを退避対象フォルダと定める設定を行

っておけばよい。そうすれば、退避処理部160が、退避対象認識処理を実行する際に、退避対象フォルダB内に格納されているファイルF1, F2, F3を退避対象ファイルと認識することができる。その結果、図3に示すような退避処理が実行されることになる。図3(a)は退避処理前のデータ格納部110の状態を示しており、図3(b)は退避処理後のデータ格納部110および外部の記憶装置300の状態を示している。図示のとおり、退避処理により、データ格納部110内のフォルダBは、そのまま外部の記憶装置300へとコピーされ、データ格納部110内からは削除されている。結局、データ格納部110には、フォルダA, Cのみが残っている。このフォルダA, C内のファイルF0, F4, F5については、他のユーザによるアクセスを受ける可能性があるが、上述したとおり、これらのファイルはセキュリティ上は問題がないファイルである。

ネットワーク200を介して外部の記憶装置300へファイルを退避する処理は、情報処理装置100にそれなりの作業負荷を与えることになる。また、後に行われる復元処理も、同様の作業負荷を与える。したがって、実用上は、セキュリティの確保が必要なファイルと、そうでないファイルとを区分けし、前者のファイルのみを退避対象ファイルとして取り扱うようにするのが好ましい。上述の例のように、予め所定のフォルダを退避対象フォルダとして定めておく方法を採用すれば、ユーザ自身の判断で退避対象ファイルの取捨選択を行うことができるので便利である。上述の例の場合、ユーザは、セキュリティの確保が必要なファイルをフォルダBに入れ、それ以外のファイルをフォルダCに入れて区別すればよい。

もちろん、退避対象ファイルの取捨選択を行う方法は、退避対象フォルダを定めておく方法に限定されるものではない。たとえば、予め定められた所定の拡張子がファイル名に付されているデータファイルを、退避対象ファイルとして認識するような方法を採用することも可能である。一般的なOSでは、個々のフ

ファイルのファイル名に、当該ファイルのフォーマットや当該ファイルを作成したアプリケーションプログラムを特定するための拡張子を付加する取り扱いは行われている。たとえば、「ABC.txt」なるファイル名における「txt」は、当該ファイルが単純なテキストファイルであることを示す拡張子である。そこで、

- 5 ユーザが、たとえば、ある特定のアプリケーションプログラムで作成したファイルを退避対象ファイルにしたいと考えた場合は、当該アプリケーションプログラムで作成したファイルに固有の拡張子をファイル名にもつファイルを、退避対象ファイルとして認識するような条件設定を行っておけば、退避処理部160によって、当該条件設定に基づく退避対象ファイルの取捨選択を自動的に
10 実行することが可能になる。

(2) 必要に応じた復元処理

- 上述した基本的な実施形態では、ユーザ甲がログオン手続を実行したときに、前回退避したファイルF1、F2、F3のすべてを直ちにデータ格納部110内に復元する例を述べたが、復元処理は必ずしもすべての退避対象ファイルに
15 対して実行する必要はなく、必要に応じて行えば足りる。たとえば、ユーザ甲のログオフ時に、図3に示す例のように、フォルダB内に格納されていた退避対象ファイルF1、F2、F3を、フォルダBごと外部の記憶装置300へ退避した場合を考えよう。この場合、このユーザ甲が、再度ログオンする際に、退避対象ファイルF1、F2、F3を、フォルダBごとそっくりデータ格納部
20 110内にコピーして復元すれば、前回のログオン時と同等の環境が復元されたことになる。しかしながら、ネットワーク200を介した復元処理は、情報処理装置100に作業負荷を加える要因になり、復元対象となるデータ容量が大きいと、復元処理時に、情報処理装置100の応答性が低下するなどの弊害を生じる可能性がある。

- 25 ここで、もし、再度ログオンしたユーザ甲が、ファイルF2に対して何らかの更新処理を実行した後にログオフしたとすると、実際に復元する必要があっ

たファイルはファイルF 2のみであり、ファイルF 1, F 3の復元処理は無駄ということになる。この場合、ユーザ甲の作業対象となるファイルF 2のみを復元すれば足りる。しかしながら、ファイルF 1, F 2, F 3の復元を全く行わない状態では、そもそもデータ格納部110内に、ファイルF 1, F 2, F 3が存在していないので、ファイルリスト上にも、ファイルF 1, F 2, F 3の存在が示されないことになり、ユーザ甲は、作業対象としてファイルF 2を指定することすらできない。すなわち、図3(b)に示すような状態のままでは、データ格納部110内には、フォルダA, Cのみしか存在していないので、図2に示すようなファイルリスト表示を行ったとしても、フォルダBや、その中に格納されているファイルF 1, F 2, F 3が表示されることはない。

このような問題を解決するためには、復元処理部170に、二段階の復元処理機能をもたせておくようにすればよい。すなわち、第1段階の復元処理機能は、データファイルの保存時の階層構造を復元する予備復元処理であり、第2段階の復元処理機能は、予備復元処理によって復元された階層構造内から選択された特定のデータファイルを実際に復元する本復元処理である。

図4は、この二段階の復元処理機能の概念を説明する図である。まず、第1段階の予備復元処理では、データファイルの保存時の階層構造のみが復元される。すなわち、図4(a)に示すように、退避対象となったフォルダBの階層構造のみの復元が行われる。図では、便宜上、階層構造のみの復元が行われたフォルダやファイルを破線のブロックで示してある。この図4(a)に示す予備復元処理の段階では、ファイルF 1, F 2, F 3の実体データの復元は行われていない。しかしながら、フォルダBの中にファイルF 1, F 2, F 3が格納されている、という階層構造（フォルダ名やファイル名も含めた階層構造）についての復元は行われているので、図2に示すようなファイルリスト表示を行った場合、フォルダBの存在や、その中にファイルF 1, F 2, F 3が格納されているという階層構造を表示させることは可能になる。

結局、予備復元処理では、ファイルF 1, F 2, F 3の実体データをデータ格納部110にコピーする必要はなく、「フォルダB」なる名前のフォルダの中に、「ファイルF 1」なる名前のファイルと、「ファイルF 2」なる名前のファイルと、「ファイルF 3」なる名前のファイルと、が格納されている、という階層構造を示す情報のみをデータ格納部110内に復元すればよいので、復元すべきデータ容量は大幅に低減される。なお、図2のウィンドウW2に示すように、各ファイルのサイズや修正日時といった書誌情報も表示させる必要がある場合には、この書誌情報も併せて復元する必要があるが、それでも復元すべきデータ容量は大幅に低減される。

- 10 このように、まず第1段階の復元処理として、予備復元処理を実行しておけば、ユーザには、とりあえず、図2に示すようなファイルリストの提示を行うことができるので、データ格納部110内に格納されているファイル構造が、あたかも前回のログオフ直前の状態と同等であるかのように見せることができる。実際、ユーザは、図2に示すようなファイルリストの表示を見て、データ
- 15 格納部110内には、3つのフォルダA, B, Cが格納されている状態を確認することができ、フォルダBの中には、ファイルF 1, F 2, F 3が格納されている状態を確認することができる。

- もっとも、この図2に示すようなファイルリスト表示は、パソコンなどの情報処理装置100に備わっているOSの標準機能では行うことができない。すなわち、データ格納部110内には、実際にフォルダB内のファイルの復元が行われているわけではなく、その階層構造を示すデータのみが所定のフォーマットで書き込まれているにすぎないので、この所定のフォーマットを解釈して、図2に示すようなウィンドウ上に階層構造をファイルリストとして表示する機能を果たす専用のアプリケーションプログラムが必要になる。したがって、復元処理部170は、このような専用のアプリケーションプログラムを含んだ構成要素ということになる。
- 20
- 25

さて、図2に示すウインドウW2上で、ユーザがファイルF2のアイコンをダブルクリックするなどして、ファイルF2をメモリ130上に展開する指示を与えたとしよう（あるいは、所定のアプリケーションプログラムから、ファイルF2を開く指示を与えても同様である）。この場合、図4(a)に示すように、

5 ファイルF2の実体は、データ格納部110にはまだ存在しないので、ファイルF2を直ちにメモリ130上に展開する処理を行うことはできない。その代わりに、復元処理部170が、ファイルF2に対する本復元処理を実行する。

すなわち、携帯可能情報記録媒体400内の管理情報を参照して、ファイルF2の退避場所アドレスを認識し、ファイルF2の実体となるデータファイルを

10 実際にデータ格納部110内へと復元する処理が実行される。図4(b)は、このような本復元処理が実行された後のデータ格納部110内の状態を示す図である。破線で示すファイルF1、F3の実体は依然として復元されていない状態であるが、実線で示すファイルF2は、その実体がデータ格納部110内に復元されることになるので、これをメモリ130上に展開することが可能になる。

15 もっとも、ユーザから見れば、単に、所望のファイルF2を所定のアプリケーションプログラムで開く作業を行っただけであり、上述した本復元処理が行われたことは、ユーザの意識する事項ではない。別言すれば、ユーザから見た操作性は、従来の一般的なパソコンに対する操作性とほぼ同じである。ここで、このユーザが、プログラム実行部150に対して所定の操作を行うことにより、

20 メモリ130上に展開されているデータファイルF2に対して、何らかの更新処理を行った後、これを保存する操作を行えば、更新後のデータファイルF2は、データ格納部110内のデータファイルF2に上書き保存されることになる。そして、このユーザが、ここでログオフ手続を行ったとすると、退避処理部160により、データ格納部110内に実在するデータファイルF2が退避
25 対象ファイルとして認識され、退避処理が実行される。そして、携帯可能情報記録媒体400内の管理情報のうち、データファイルF2の退避場所アドレス

が書き換えられることになる。

このような運用を行えば、実際に復元する必要があったデータファイルF2
に対してのみ本復元処理が実行されることになり、ログオフ時には、当該デー
タファイルF2に対してのみ退避処理が実行されることになるので、全データ
5 ファイルを一括して復元し、一括して退避する方法に比べて、より効率的な運
用が可能になる。

(3) 退避対象ファイルの分割処理および暗号化処理

本発明による退避処理が行われると、情報処理装置100内には退避対象フ
ァイルは残っていないので、情報処理装置100に関する限り、十分なセキュ
10 リティが確保されることになる。しかしながら、退避対象ファイルは、外部の
記憶装置300に格納されているため、この外部の記憶装置300に対するア
クセスにより、セキュリティが破られるおそれがある。もっとも、実用上は、
ネットワーク200としてインターネットを用いるようにすれば、外部の記憶
装置300は、インターネットに接続された任意の記憶装置によって構成する
15 ことができるため、特定の退避対象ファイルの退避場所を知ることは、携帯可
能情報記録媒体400内の管理情報を参照しない限り、事実上不可能である。
したがって、個々のユーザが、それぞれ所持する携帯可能情報記録媒体400
をしっかりと管理していれば、退避対象ファイルの退避場所が外部に漏えいす
る危険性は低い。特に、携帯可能情報記録媒体400としてICカードを利用
20 すれば、内部に保存した管理情報が不正な手段で外部に読み出される可能性は
極めて低い。

しかしながら、外部の記憶装置300は、インターネットに接続された環境
にあるため、何者かによる直接攻撃の対象になるおそれがあり、退避対象フ
ァイルが、そのまま不正な手段で外部へ読み出される可能性がある。このような
25 問題に対処するためには、退避対象ファイルに対して分割処理を施したり、暗
号化処理を施したりするのが好ましい。以下、このような対策を具体例に即し

て説明する。

図5は、退避対象ファイルに対する分割処理の概念を示す図である。ここでは、退避対象となったファイルF2に対して分割処理を行う一例が示されている。すなわち、この例では、データ格納部110内のファイルF2を退避する
5 際に（外部の記憶装置にコピーする際に）、退避処理部160によって、ファイルF2を3つの分割ファイルF2a、F2b、F2cに分割する処理が実行される。そして、この3つの分割ファイルF2a、F2b、F2cが、ネットワーク200を介して、それぞれ異なる外部の記憶装置に退避される。

図6は、3つの分割ファイルF2a、F2b、F2cを、それぞれ異なる記憶装置に退避するために、ネットワーク200に3つの異なる記憶装置を接続した変形例を示すブロック図である。図1に示す基本的な実施形態と、この図
10 6に示す変形例との相違は、後者では、退避場所として第1の記憶装置310、第2の記憶装置320、第3の記憶装置330が用意されている点と、退避処理部160が分割処理を行う点と、復元処理部170が分割ファイルを合成し
15 て復元処理を行う点である。

そこで、以下、図6を参照しながら、退避処理部160による退避処理と、復元処理部170による復元処理とが、どのように行われるかを説明する。ここでは、便宜上、ログオン中のユーザ甲がログオフ手続を行った時点で、データ格納部110内には、図示のとおり、3つのデータファイルF1、F2、F
20 3が格納されており、そのうちデータファイルF2が退避対象ファイルとなっていたという前提で、以下の説明を行うことにする。

ユーザ甲がログオフ手続を行うと、既に述べたとおり、退避処理部160によって、5つの処理が実行される。すなわち、この例の場合、まず、退避対象認識処理により、データ格納部110内のデータファイルF2が退避対象ファ
25 イルとして認識される。続いて、退避処理が行われるが、このとき、データファイルF2に対する分割処理が行われ、データファイルF2は複数の分割ファ

イルに分割された状態で、外部の記憶装置へとコピーされることになる。具体的には、図5に示す例では、ファイルF2は、3つの分割ファイルF2a, F2b, F2cに分割され、それぞれ第1の記憶装置310, 第2の記憶装置320, 第3の記憶装置330へとコピーされることになる。

- 5 この退避処理が完了したら、データ格納部110内のデータファイルF2を削除する削除処理が行われる。そして、管理情報作成処理が行われ、作成された管理情報を携帯可能情報記録媒体400に保存する管理情報保存処理が行われる。この変形例の場合、データファイルF2について作成される管理情報について留意すべき点が2つある。
- 10 第1点は、ファイルF2の退避場所を示すアドレスとして、個々の分割ファイルF2a, F2b, F2cのそれぞれの退避場所となった3ヶ所のアドレスを、管理情報に含ませておく点である。具体的には、第1の記憶装置310内の分割ファイルF2aの格納先を示すURLアドレスと、第2の記憶装置320内の分割ファイルF2bの格納先を示すURLアドレスと、第3の記憶装置
- 15 330内の分割ファイルF2cの格納先を示すURLアドレスと、が管理情報として用意されることになる。そもそも本発明における管理情報とは、外部の記憶装置に退避された退避対象ファイルをデータ格納部110内にコピーして復元するために必要な情報であるから、退避対象ファイルF2が3つに分割され、それぞれ異なる場所に退避されたのであれば、個々の分割ファイルの退避
- 20 場所アドレスを管理情報として用意するのは当然である。

- 第2点は、退避対象ファイルF2に対して施した分割処理の方法を示す情報を、管理情報に含ませておく点である。たとえば、図5に示す分割処理は、「退避対象ファイルF2を3つに等分割し、先頭から順に、分割ファイルF2a, F2b, F2cとする」という分割方法によって行われることになるので、当
- 25 該分割方法を示す情報を管理情報に含ませておくようにする。そうすれば、後に復元処理部170による復元処理を行う際に、管理情報内の分割方法を示す

情報を参照することにより、分割ファイルF 2 a, F 2 b, F 2 cを合成して、元のデータファイルF 2を復元することが可能になる。

- 結局、この分割処理を施す変形例では、退避処理部1 6 0は、退避処理を実行する際に、退避対象ファイルを所定の分割方法に基づいて複数の分割ファイルに分割し、個々の分割ファイルをそれぞれ異なる複数の記憶装置に退避させる処理を実行し、実施した分割方法を示す情報を含む管理情報を作成するようにし、復元処理部1 7 0は、この管理情報に含まれている分割方法を示す情報に基づいて、退避対象ファイルの復元を行うようにすればよい。

- この変形例のメリットは、外部の記憶装置へ退避される退避対象ファイルが、そのままの形ではなく、複数の分割ファイルとして、ばらばらに格納される点にある。たとえば、上述の例の場合、データファイルF 2は、3つの分割ファイルF 2 a, F 2 b, F 2 cに分割された上、3ヶ所に分散して格納されることになるので、万一、いずれかの分割ファイルが不正な手段でアクセスされたとしても、もとのデータファイルF 2自身が直ちに露見することは防げる。

- この変形例において、セキュリティの効果をできるだけ高めるには、より複雑な分割方法を採用するようにすればよい。たとえば、図5に示す例では、元のファイルF 2を3等分するという単純な分割方法を採用しているため、万一、分割ファイルF 2 a, F 2 b, F 2 cのすべてが不正な手段によって入手されてしまうと、これらをこの順に合成することにより、元のファイルF 2を復元することが可能になる。これに対して、たとえば、同じ3つのファイルに分割する方法でも、元のファイルF 2を構成するバイト列の先頭から、1, 4, 7, 1 0, …バイト目というように3バイト周期で1バイトずつを抜き出すことにより第1の分割ファイルF 2 aを作成し、2, 5, 8, 1 1, …バイト目というように3バイト周期で1バイトずつを抜き出すことにより第2の分割ファイルF 2 bを作成し、3, 6, 9, 1 2, …バイト目というように3バイト周期で1バイトずつを抜き出すことにより第3の分割ファイルF 2 cを作成する、

という分割方法を採用した場合、このような分割方法が行われたことを知らない者にとっては、3つの分割ファイルF2a, F2b, F2cを入手できたとしても、元のファイルF2を復元することは困難になる。

実際には、このような分割方法の原理は無限に存在し、また、同じ原理に基づく分割方法でも、パラメータ値を種々変えることにより、実質的には異なる分割方法になる。したがって、退避処理部160内に予め複数通りの分割方法を定義しておき、更に、パラメータをランダムに設定するようにすれば、実質的に無限通りの分割方法の中の1つを選択することができるので、退避対象ファイルごとに、それぞれ異なる分割方法を適用して退避させることが可能になる。

また、図6では、外部の記憶装置として、3つの記憶装置310, 320, 330を用いる例を示したが、ネットワーク200としてインターネットを用いるようにすれば、これら外部の記憶装置は、理論上無限に設置することができる。したがって、これら外部の記憶装置のそれぞれが、不正な手段でアクセスされる可能性があったとしても、特定の退避対象ファイルが、どのような分割方法でいくつに分割され、その結果として生成された個々の分割ファイルがどの記憶装置のどのアドレスに格納されたか、という事項を示す管理情報（これは、ユーザが所持する携帯可能情報記録媒体400内にのみ保存されている）がない限り、第三者が退避対象ファイルを復元することは不可能である。

このような分割処理と同様にセキュリティ確保に有効な手段は、暗号化処理である。すなわち、退避処理部160が、退避処理を実行する際に、退避対象ファイルを所定の暗号化方法に基づいて暗号化した上で外部の記憶装置に退避させる処理を実行し、当該暗号化方法を示す情報を含む管理情報を作成するようにし、復元処理部170が、退避対象ファイルの復元を行う際に、この管理情報に含まれている暗号化方法を示す情報に基づいて復号化処理を実行するようにすればよい。

たとえば、データファイルF2が退避対象である場合、このデータファイルF2に対して、所定の暗号化プロセスを施して、暗号化ファイルFF2を生成し、この暗号化ファイルFF2を外部の記憶装置へコピーして格納すればよい。このとき、どのような暗号化プロセスを施したかを示す情報（暗号化のために何らかのキーを用いた場合には、当該キーも含めた情報）を、管理情報に含めておくようにする。そうすれば、万一、外部の記憶装置に格納されている暗号化ファイルFF2が不正にアクセスされたとしても、暗号解読ができない限り、セキュリティ上の支障は生じない。もちろん、正規のユーザがログオンしたときには、携帯可能情報記録媒体400内の管理情報に含まれている暗号化方法を示す情報に基づいて、暗号化ファイルFF2に対する復号化処理を行うことができるので、元のデータファイルF2を復元することが可能である。

もちろん、より高いセキュリティを確保するために、分割化処理と暗号化処理とを組み合わせることも可能である。たとえば、退避対象ファイルを分割して複数の分割ファイルを生成した後、個々の分割ファイルのそれぞれに対して暗号化処理を施した上で、外部の記憶装置へと退避させるようなことも可能であるし、逆に、退避対象ファイルを暗号化した上で、この暗号化されたファイルを分割して複数の分割ファイルを生成し、これらを外部の記憶装置へと退避させるようなことも可能である。

(4) 管理情報の保存場所

本発明を実施する上で、管理情報は重要な役割を果たす。すなわち、管理情報は、外部の記憶装置へ退避した退避対象ファイルを復元するために必要な情報であり、復元処理部170による復元処理に不可欠の情報である。その半面、この管理情報が、他のユーザの手に入ってしまうと、当該他のユーザによっても、退避対象ファイルの復元が可能になってしまうため、セキュリティ確保の観点からは、この管理情報は、情報処理装置100の内部ではなく、外部の記憶場所に保存する必要がある。

そこで、これまで述べた実施形態では、情報処理装置100に対して着脱自在な携帯可能情報記録媒体400を管理情報の記憶場所とするようにし、退避処理部160が管理情報を保存する際には、この携帯可能情報記録媒体400を保存場所とし、復元処理部170が復元処理を行う際には、この携帯可能情報記録媒体400に保存されている管理情報を参照した復元が行われるようにしている。特に、上述した実施形態では、ICカードを携帯可能情報記録媒体400として用いる運用を行っている。具体的には、予め、個々のユーザごとにそれぞれ固有のICカードを発行しておき、ログイン処理を行う際には、必ずこのICカードをリーダライタ装置に挿入させるようにし、ログオフ処理を行った後は、必ずこのICカードをリーダライタ装置からエジェクトして携帯させるような運用を行っている。

しかしながら、本発明を実施する上では、管理情報は必ずしもICカードのような携帯可能情報記録媒体400に保存する必要はない。すなわち、管理情報は、情報処理装置100の外部に存在し、正規のユーザによるアクセスのみが可能となるような環境下にある記憶場所に保存できれば、必ずしも携帯可能情報記録媒体400に保存する必要はない。具体的には、たとえば、管理情報を、ネットワーク200を介して接続された外部のサーバ装置などに保存するようにし、保存先のURLアドレスを正規のユーザに対してのみ知らせておくような運用を採ることも可能である。この場合、ユーザは、ログオン時に当該URLアドレスを入力する操作を行えばよい。復元処理部170は、この入力されたURLアドレスに存在する管理情報を参照することにより、必要なファイルの復元処理を行うことができる。

(5) 情報処理装置100の具体的な構築方法

実用上、図1に示す情報処理装置100として機能する代表的な装置はパソコンである。既に§1で述べたとおり、この図1のブロック図に示す構成要素のうち、データ格納部110、展開保存部120、メモリ130、ユーザ管理

部 1 4 0、プログラム実行部 1 5 0 なる構成要素によって実現される機能は、現在市販されている一般的なパソコン（所定の OS が組み込まれたパソコン）に標準的に備わっている機能である。したがって、このような市販のパソコンを、本発明に係る情報処理装置 1 0 0 として利用するには、このパソコンに、

5 退避処理部 1 6 0 および復元処理部 1 7 0 としての機能を追加し、携帯可能情報記録媒体 4 0 0 などの管理情報の記憶場所を準備すればよい。ここで、退避処理部 1 6 0 および復元処理部 1 7 0 としての機能は、プログラムによって実現できるので、結局、実用上は、市販の汎用パソコンに、退避処理部 1 6 0 および復元処理部 1 7 0 としての機能を果たす専用のプログラムを組み込むこと

10 により、本発明に係るデータ格納部 1 1 0 を構成することが可能である。もちろん、この専用のプログラムは、CD-ROM などのコンピュータ読取り可能な記録媒体に記録して配付することも可能であるし、オンラインで配付することも可能である。

このように、本発明に係る情報処理装置は、汎用パソコンに専用プログラム

15 を組み込むことにより実現できる装置なので、企業などで本発明に係る情報処理装置を利用する場合、実用上は、複数の情報処理装置を同時に導入し、並列的に運用する形態が一般的になるものと予想される。この場合、退避対象ファイルについての復元処理は、必ずしも当該ファイルについての退避処理を行った同一の情報処理装置で行う必要はない。

20 たとえば、図 1 に示すような情報処理装置 1 0 0 として機能するパソコンが、東京本社に設置されるとともに、大阪支社にも設置されたとしよう。この場合、東京本社の社員であるユーザ甲が、東京本社に設置されている情報処理装置 1 0 0（東京）にログオンし、データファイル F 2 を作成する作業を行い、ログオフする際に、当該データファイル F 2 が退避対象ファイルとして、外部の記憶装置 3 0 0 へ退避されたものとしよう。この場合、このユーザ甲が、後日、

25 再び情報処理装置 1 0 0（東京）にログオンすれば、データファイル F 2 は、

この情報処理装置100（東京）内に復元されることになる。しかし、このユーザ甲が、大阪に出張した際に、大阪支社に設置されている情報処理装置100（大阪）にログオンすれば、データファイルF2は、この情報処理装置100（大阪）内に復元されることになる。

- 5 要するに、ユーザ甲が作成したデータファイルF2の退避処理に関する情報は、ユーザ甲の所持する携帯可能情報記録媒体400内に管理情報として保存されているので、ユーザ甲は、この携帯可能情報記録媒体400を携帯している限り、どの情報処理装置を用いても、データファイルF2の復元が可能になる。実際、ネットワーク200としてインターネットを用いるようにすれば、
- 10 外部の記憶装置300に対しては、世界中のどこからでもアクセスすることが可能になるので、ユーザ甲は、ニューヨーク支社に設置された情報処理装置100（Newyork）にログオンしてデータファイルF2を復元することも可能になるし、ロンドン支社に設置された情報処理装置100（London）にログオンしてデータファイルF2を復元することも可能になる。このように、自分が作成したデータファイルを、どこからでも利用することができるようになる、という効果は、セキュリティを確保するという目的を達成するために生まれた本発明の副次的な効果というべきものである。
- 15

産業上の利用可能性

- 20 本発明は、パソコンなどの情報処理装置を、複数のユーザによって共有して利用する場合に広く利用することができる。特に、複数ユーザによって共有されている情報処理装置において、個々のユーザが作成したデータについて十分なセキュリティを確保する環境で利用するのに最適である。

請 求 の 範 囲

1. データファイルを格納するためのデータ格納部（110）と、

前記データ格納部に格納されているデータファイルを必要に応じて展開する
5 ためのメモリ（130）と、

複数のユーザによる重複ログオンが行われることがないように、所定のユーザによるログオン手続が行われた後は、当該ユーザについてのログオフ手続が行われるまで、他のユーザによるログオン手続を拒絶するユーザ管理部（140）と、

10 ログオン中のユーザの操作に基づいて、前記データ格納部（110）に格納されている所定のデータファイルを前記メモリ（130）上に展開するファイル展開処理と、前記メモリ（130）上に展開されている所定のデータファイルを前記データ格納部（110）に格納するファイル保存処理と、を実行する展開保存部（120）と、

15 ログオン中のユーザの操作に基づいて、所定のアプリケーションプログラムを実行し、前記メモリ（130）上に新たなデータファイルを作成する処理もしくは前記メモリ（130）上に展開されている既存のデータファイルに対する更新処理を実行するプログラム実行部（150）と、

特定のユーザがログオフ手続を実行したときに、前記データ格納部（110）
20 に格納されているデータファイルのうち、当該特定のユーザの作業に基づいて作成もしくは更新されたデータファイルの全部もしくは所定の一部を退避対象ファイルとして認識する退避対象認識処理と、前記退避対象ファイルをネットワーク（200）を介して外部の記憶装置（300）にコピーすることにより退避させる退避処理と、前記データ格納部（110）内に格納されている前記
25 退避対象ファイルを削除する削除処理と、前記外部の記憶装置（300）に退避された退避対象ファイルを前記データ格納部（110）内にコピーして復元

するために必要な管理情報を作成する管理情報作成処理と、作成した管理情報を外部の記憶場所（４００）に保存する管理情報保存処理と、を実行する退避処理部（１６０）と、

- 前記特定のユーザがログオン手続を実行した後、必要に応じて、前記管理情報
- 5 報を参照することにより、前記外部の記憶装置（３００）に退避されている退避対象ファイルを前記データ格納部（１１０）内にコピーして復元する復元処理を実行する復元処理部（１７０）と、

を備えることを特徴とする情報処理装置（１００）。

- 10 2. 請求項１に記載の情報処理装置（１００）において、

復元処理部（１７０）が、データファイルの保存時の階層構造を復元する予備復元処理と、この予備復元処理によって復元された階層構造内から選択された特定のデータファイルを復元する本復元処理と、を実行することを特徴とする情報処理装置。

15

3. 請求項１または２に記載の情報処理装置（１００）において、

退避処理部（１６０）が、予め定められた退避対象フォルダ内に格納されているデータファイルを、退避対象ファイルとして認識することを特徴とする情報処理装置。

20

4. 請求項１または２に記載の情報処理装置（１００）において、

退避処理部（１６０）が、予め定められた所定の拡張子がファイル名に付されているデータファイルを、退避対象ファイルとして認識することを特徴とする情報処理装置。

25

5. 請求項１～４のいずれかに記載の情報処理装置（１００）において、

退避処理部（１６０）が、管理情報保存処理を実行する際に、着脱自在な携帯可能情報記録媒体（４００）に管理情報を保存し、

復元処理部（１７０）が、復元処理を実行する際に、前記携帯可能情報記録媒体（４００）に保存されている管理情報を参照することを特徴とする情報処理装置。

６． 請求項１～５のいずれかに記載の情報処理装置（１００）において、
管理情報として、退避対象ファイルの退避先となる外部の記憶装置のアドレス情報を用いることを特徴とする情報処理装置。

７． 請求項１～６のいずれかに記載の情報処理装置（１００）において、
退避処理部（１６０）が、退避処理を実行する際に、退避対象ファイルを所定の分割方法に基づいて複数の分割ファイルに分割し、個々の分割ファイルをそれぞれ異なる複数の記憶装置（３１０，３２０，３３０）に退避させる処理
を実行し、前記所定の分割方法を示す情報を含む管理情報を作成する機能を有し、

復元処理部（１７０）が、前記管理情報に含まれている前記所定の分割方法を示す情報に基づいて、退避対象ファイルの復元を行うことを特徴とする情報処理装置。

８． 請求項１～７のいずれかに記載の情報処理装置（１００）において、
退避処理部（１６０）が、退避処理を実行する際に、退避対象ファイルを所定の暗号化方法に基づいて暗号化した上で外部の記憶装置（３００）に退避させる処理を実行し、前記所定の暗号化方法を示す情報を含む管理情報を作成する機能を有し、

復元処理部（１７０）が、前記管理情報に含まれている前記所定の暗号化方

法を示す情報に基づいて復号化処理を実行し、退避対象ファイルの復元を行うことを特徴とする情報処理装置。

9. 請求項1～8のいずれかに記載の情報処理装置（100）において、

- 5 退避処理部（160）が、削除処理を実行する際に、メモリに展開されている退避対象ファイルに対しても削除する処理を行うことを特徴とする情報処理装置。

10. 請求項1～9のいずれかに記載の情報処理装置（100）としてコン

- 10 ピュータを機能させるコンピュータプログラムまたは当該プログラムを記録したコンピュータ読取り可能な記録媒体。

11. データファイルを格納するためのデータ格納部（110）と、

前記データ格納部に格納されているデータファイルを必要に応じて展開する

- 15 ためのメモリ（130）と、

複数のユーザによる重複ログオンが行われないように、所定のユーザによるログオン手続が行われた後は、当該ユーザについてのログオフ手続が行われるまで、他のユーザによるログオン手続を拒絶するユーザ管理部（140）と、

- 20 ログオン中のユーザの操作に基づいて、前記データ格納部（110）に格納されている所定のデータファイルを前記メモリ（130）上に展開するファイル展開処理と、前記メモリ（130）上に展開されている所定のデータファイルを前記データ格納部（110）に格納するファイル保存処理と、を実行する展開保存部（120）と、

- 25 ログオン中のユーザの操作に基づいて、所定のアプリケーションプログラムを実行し、前記メモリ（130）上に新たなデータファイルを作成する処理も

しくは前記メモリ（１３０）上に展開されている既存のデータファイルに対する更新処理を実行するプログラム実行部（１５０）と、

を備える情報処理装置（１００）を、複数のユーザで共用する場合に、個々のユーザごとにデータのセキュリティを確保する方法であって、

- 5 特定のユーザがログオフ手続を実行したときに、前記データ格納部（１１０）に格納されているデータファイルのうち、当該特定のユーザの作業に基づいて作成もしくは更新されたデータファイルの全部もしくは所定の一部を退避対象ファイルとして認識する退避対象認識処理と、前記退避対象ファイルをネットワーク（２００）を介して外部の記憶装置（３００）にコピーすることにより
- 10 退避させる退避処理と、前記データ格納部（１１０）内に格納されている前記退避対象ファイルを削除する削除処理と、前記外部の記憶装置（３００）に退避された退避対象ファイルを前記データ格納部（１１０）内にコピーして復元するために必要な管理情報を作成する管理情報作成処理と、作成した管理情報を外部の記憶場所（４００）に保存する管理情報保存処理と、を実行する退避
- 15 処理段階と、

前記特定のユーザがログオン手続を実行した後、必要に応じて、前記管理情報を参照することにより、前記外部の記憶装置（３００）に退避されている退避対象ファイルを前記データ格納部（１１０）内にコピーして復元する復元処理を実行する復元処理段階と、

- 20 を前記情報処理装置（１００）に行わせることを特徴とする情報処理装置におけるセキュリティ確保方法。

１２． 請求項１１に記載のセキュリティ確保方法において、

- 25 復元処理段階が、データファイルの保存時の階層構造を復元する予備復元段階と、この予備復元段階によって復元された階層構造内から選択された特定のデータファイルを復元する本復元段階と、によって構成されることを特徴とす

る情報処理装置におけるセキュリティ確保方法。

13. 請求項11または12に記載のセキュリティ確保方法における退避処理段階および復元処理段階をコンピュータに実行させるコンピュータプログラム
- 5 ムまたは当該プログラムを記録したコンピュータ読取り可能な記録媒体。

要 約 書

- 情報処理装置（１００）にログオン中のユーザがログオフ手続を実行すると、退避処理部（１６０）により以下の処理が実行される。まず、データ格納部（１
- 5 １０）内に残っているファイルの中から、セキュリティ確保が必要なファイルとして認識された退避対象ファイルが、ネットワーク（２００）を介して外部の記憶装置（３００）へコピーされ、データ格納部（１１０）内の元のファイルは削除される。このとき、コピー先のアドレスが管理情報として、当該ユーザの所持する携帯可能情報記録媒体（４００）に保存される。当該ユーザが、
- 10 再び情報処理装置（１００）にログオンすると、復元処理部（１７０）が、携帯可能情報記録媒体（４００）内の管理情報に基づいて、外部の記憶装置（３００）へ退避されていたファイルをデータ格納部（１１０）内に復元する。同一の情報処理装置を複数のユーザで共有する場合に、十分なセキュリティを確保できる。

図 1

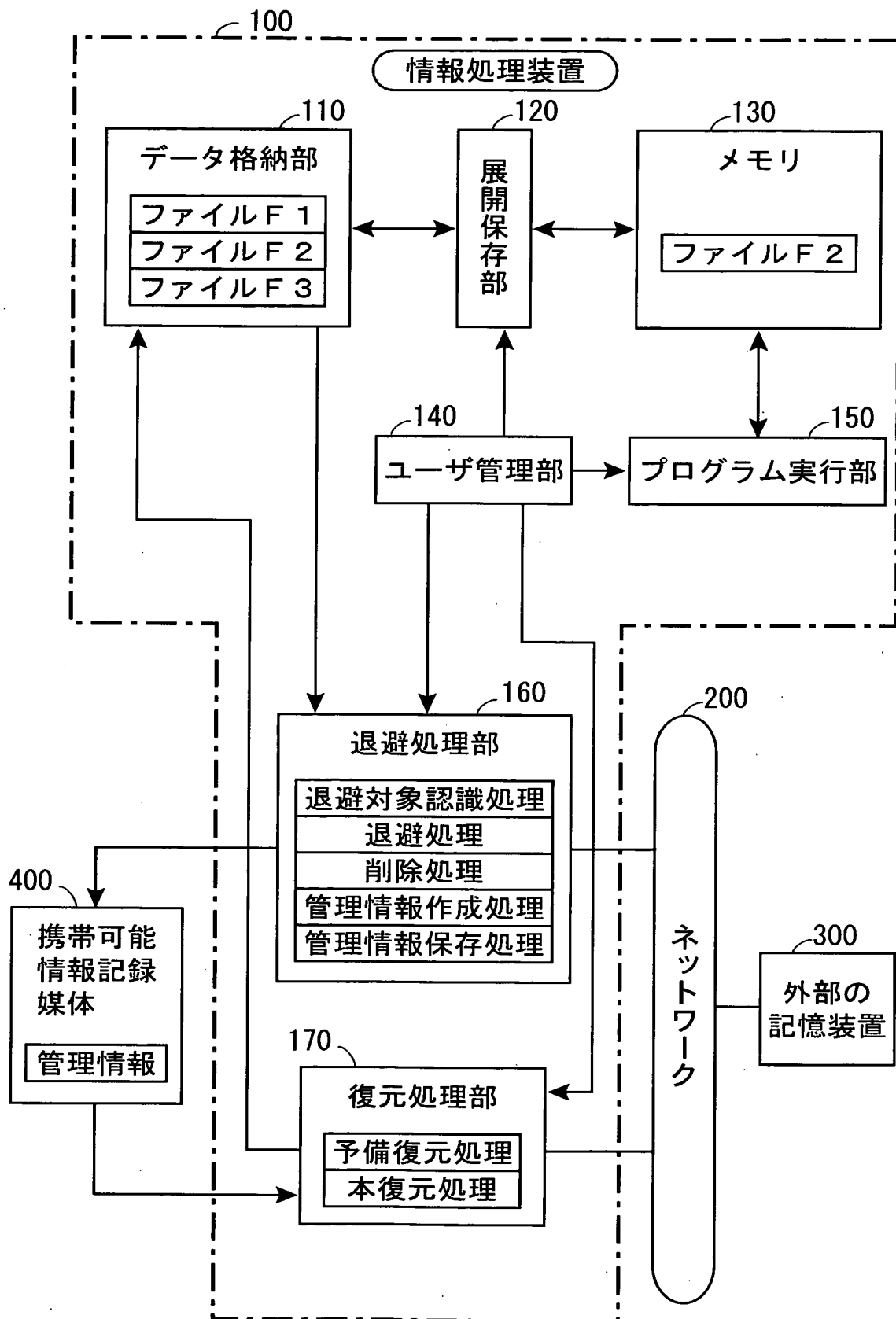


図 2

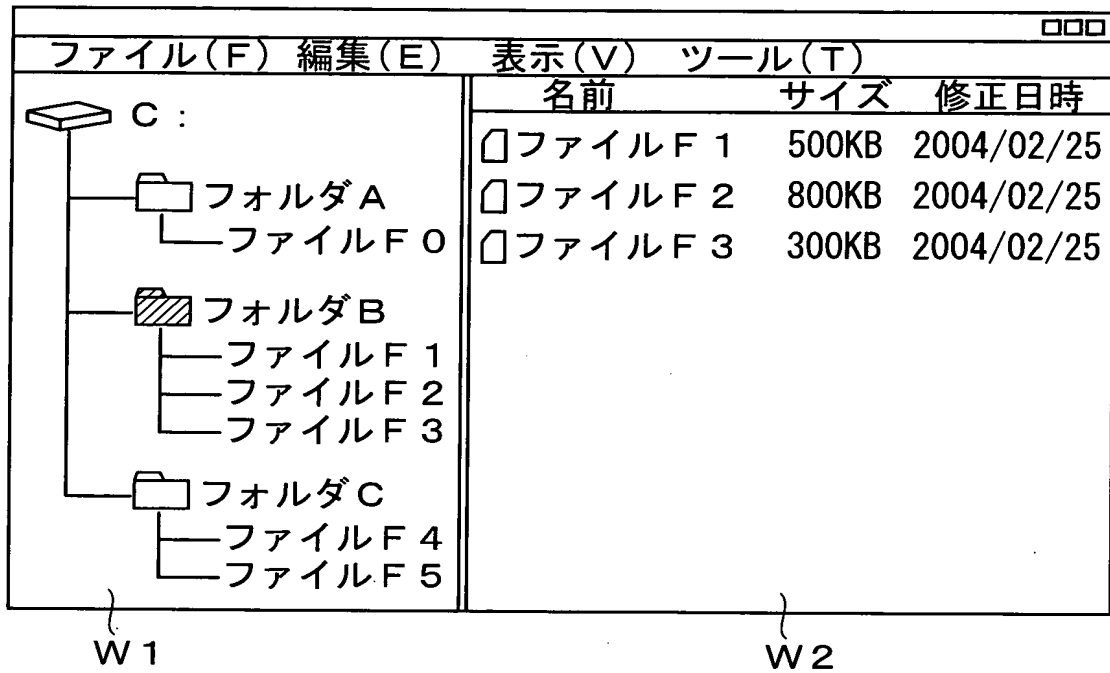


図 3

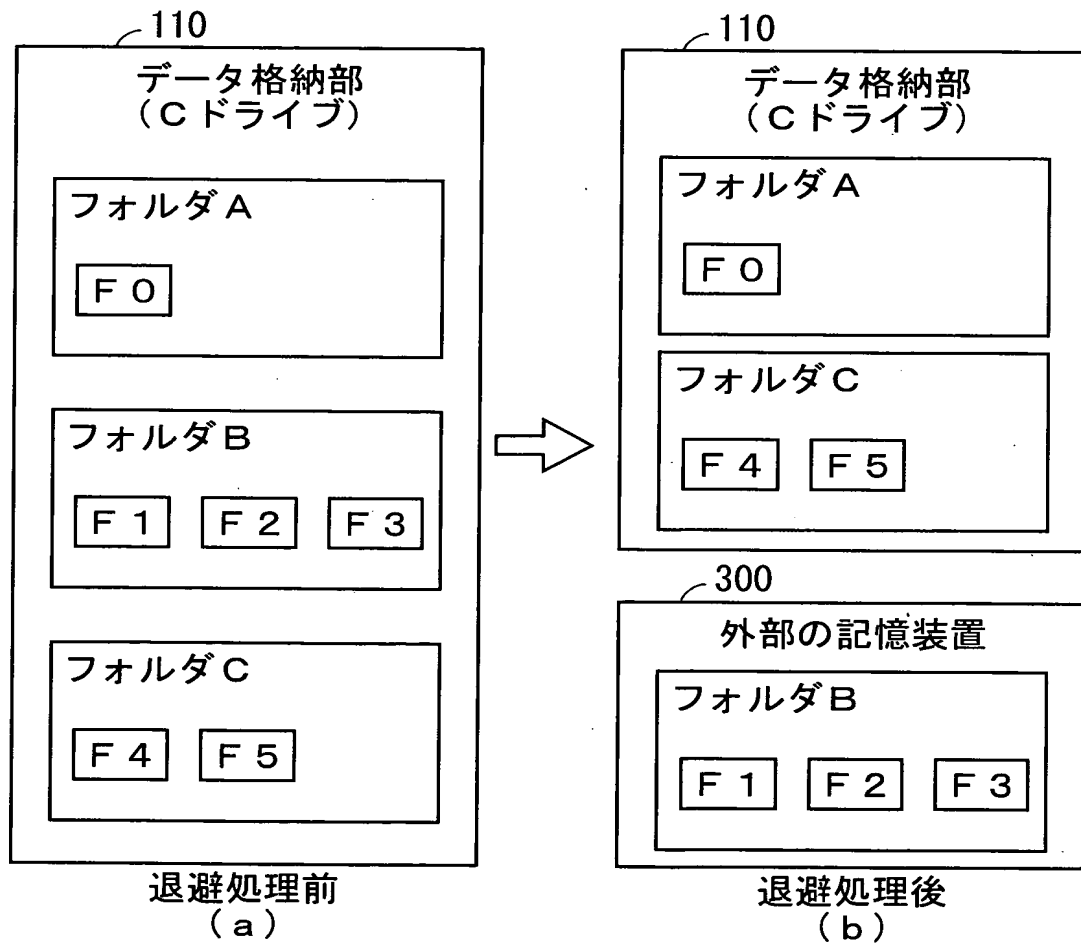


図 4

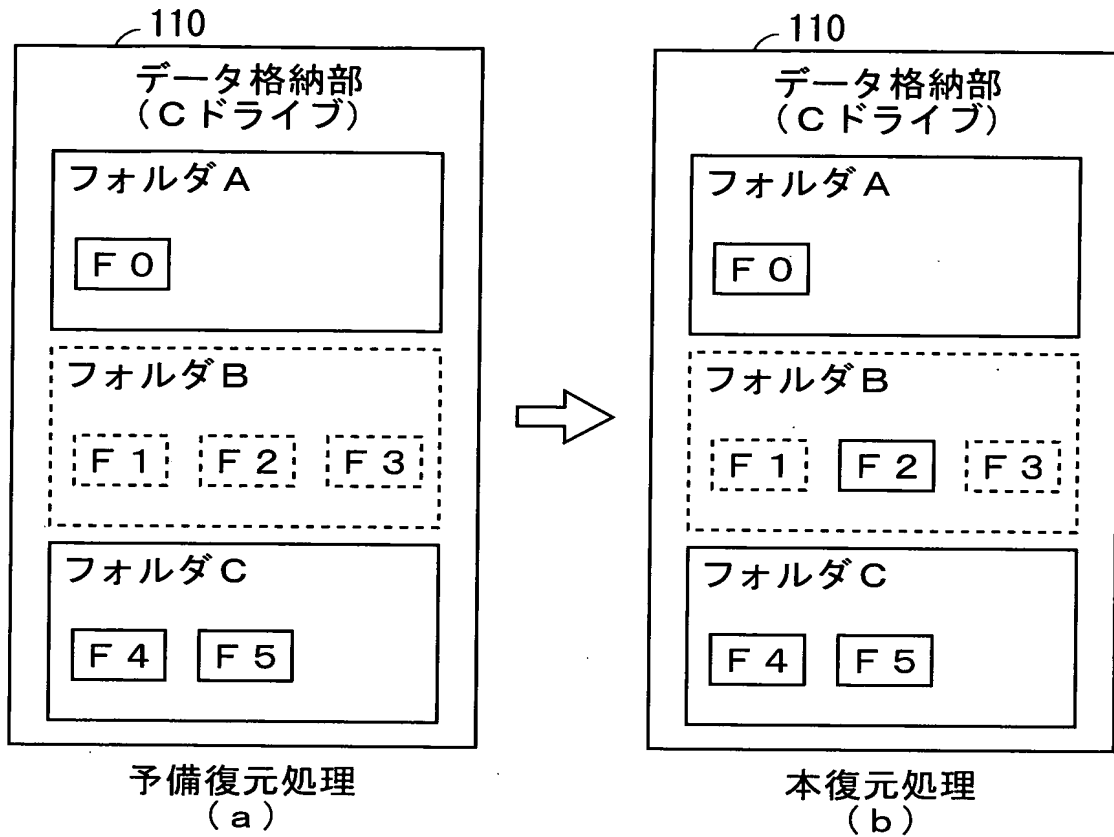


図 5

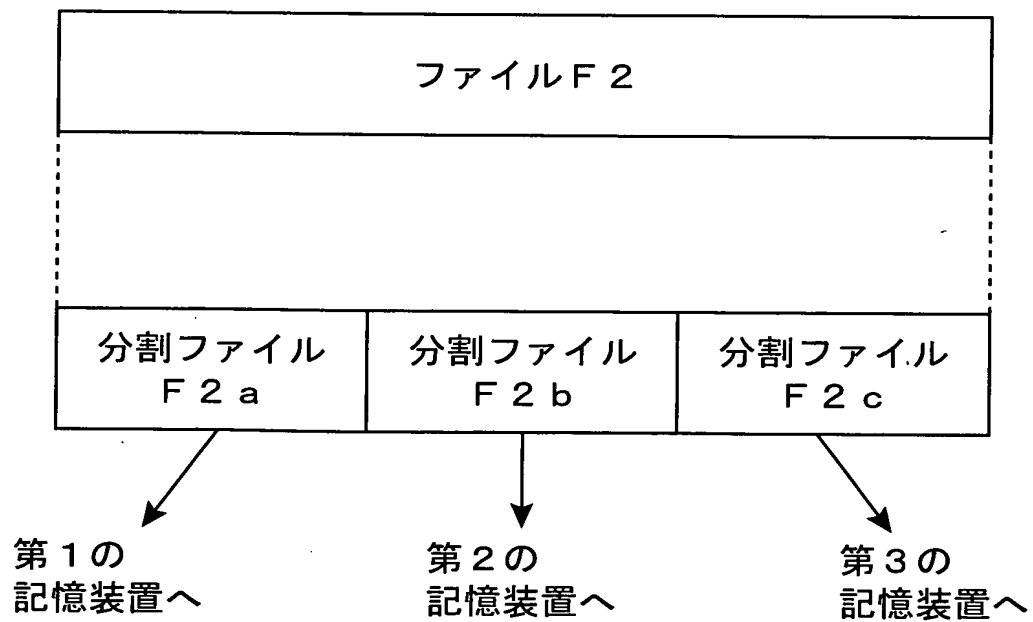


図 6

